

FILED
JUL 16 2010
WILLIAM B. GUTHRIE
Clerk, U.S. District Court
By Deputy Clerk

3. DISH Network is a limited liability company organized under the laws of the State of Colorado.
4. EchoStar Technologies is a limited liability company organized under the laws of the State of Texas.

5. Troy Phillips is an adult individual who resides in Durant, Oklahoma.

JURISDICTION AND VENUE

6. This Court has original subject matter jurisdiction over this action under 28 U.S.C. § 1331 because the claims asserted herein arise under Federal laws; specifically, the Federal Communications Act of 1934, as amended, 47 U.S.C. § 605, and the Digital Millennium Copyright Act, 17 U.S.C. § 1201 *et seq.* This Court also has supplemental jurisdiction over the Oklahoma claims asserted herein.
7. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial portion of the events giving rise to the claim occurred in this District and because the Defendant resides in this District.

BACKGROUND

Plaintiffs' Satellite Television Broadcasting and Equipment Business

8. The Plaintiff, DISH Network, is a direct broadcast satellite system television company operating throughout the United States, including the Eastern District of Oklahoma, providing state of the art satellite entertainment programming services. DISH Network provides hundreds of channels of digital entertainment and information programming to consumers, commercial establishments, hotels, motels, and others who are equipped with specialized digital satellite system equipment. DISH Network provides different levels of programming based upon the particular subscription package that a subscriber purchases.
9. DISH Network scrambles or encrypts its satellite transmissions and employs technology specifically designed to limit programming access to only those lawful subscribers who pay for its services. The technology particularly relies on conditional access security devices known as "smart cards" which, upon activation by DISH Network, unscramble

or decrypt certain DISH Network satellite signals and permit subscribers to view only the programming they are specifically authorized to receive. These “smart cards” are but one of the security measures employed by DISH Network to protect its programming against unauthorized access.

10. A legitimate consumer wishing to subscribe to and receive programming through a paid DISH Network account would utilize certain necessary equipment, which consists of primarily of:
 - a. a satellite dish antenna (“dish”), designed and/or manufactured and/or distributed by EchoStar Technologies;
 - b. an integrated receiver/decoder (“IRD” or “receiver”), designed and/or manufactured and/or distributed by EchoStar Technologies; and
 - c. a credit card-sized EchoStar Technologies access card or an internalized access card on some newer model receivers, containing encryption technology and the authorization data associated with the subscribers paid account.

Using this technology DISH Network offers a wide variety of programming, including all the major television network broadcasts, studio movies, and special events offered on a pay-per-view basis, local network television channels in some areas, international programming, sporting events, special interest programming, and the like.

Plaintiffs’ Signal Security and Piracy

11. DISH Network delivers its satellite television programming from its earth-based uplink centers which first compress, scramble and digitize programming signals before transmitting the signals to satellites located in orbit above the Earth. These transmissions are private communications and are not transmitted for the benefit or use by the general public, but are intended only for use by DISH Network’s legitimate subscribers. No

person or entity may lawfully intercept, exhibit or otherwise use DISH Network's transmissions without its express authorization.

12. DISH Network's satellite-delivered signals can be received by its subscribers by using an EchoStar Technologies satellite reception dish and receiver. The signals are then transmitted to the integrated receiver descrambler (IRD). The IRD functions as an electronic gate which processes the incoming signals using a conditional access security device, which in turn authorizes the scrambled signal to be descrambled for viewing by authorized subscribers.
13. The conditional access security device or "smart card" used by DISH Network's secure transmission system was developed to ensure that only lawful customers would be able to unscramble its signals and view its programming.
14. The "smart card" blocks access to DISH Network's programming until the subscriber purchases one or more programming packages. When the customer subscribes to a DISH Network programming package, DISH Network electronically activates the subscriber's "smart card" in accordance with that level of subscription. The "smart card" then acts as a re-programmable microprocessor to control which DISH Network programming the subscriber is permitted to view and to capture and transmit to DISH Network the subscribers' pay-per-view ("PPV") information.
15. Despite the Plaintiffs' concerted efforts to preserve the integrity of DISH Network's signals there have been and still are technologies which allow for the unauthorized decryption (theft) of DISH Network's signals. The unauthorized interception of programming through the unauthorized decryption of satellite television signals is commonly referred to in the industry as "satellite piracy" (or "piracy"). Individuals who engage in the unauthorized interception of signals are commonly referred to in the

industry as "pirates".

16. A number of years ago pirates discovered a "work around" which allowed the compromising of earlier versions of DISH Network's security encryption system and the unauthorized decryption of DISH Network's signals. The pirate community referred to this earlier version of the encryption technology as the encryption technology associated with the "Nagra 2" or "N2" generation of smart cards and the pirates sometimes imprecisely referred to this "work around" as a "card hack".
17. Through utilization of this card hack the pirates were able to decrypt DISH Network's signals without authorization until the middle of June 2009 when the Plaintiffs fully implemented their utilization of next generation of smart cards, referred to by the pirate community as "Nagra 3" or "N3" smart cards and when the encryption technology utilized by these new smart cards new cards disabled piracy devices and piracy software that were based upon the "N2" card hack.
18. One of the more common piracy methods based upon the "N2" card hack was the so-called "modified FTA" piracy method. In this type of piracy FTA receivers were programmed with N2 card hack piracy software ("modified FTA card hack software"). Once an FTA receiver had been programmed ("modified") it could decrypt DISH Network signals without authorization. An FTA receiver that has been programmed with modified FTA card hack software is often referred to as a "modified FTA receiver".
19. FTA receivers are somewhat similar in appearance to EchoStar Technologies' receivers. True FTA receivers were not originally intended for use in decrypting signals without authorization. At their earliest inception, true FTA receivers were intended to be utilized for the viewing of satellite signals which were not encrypted

and which were not subject to a marketing scheme on the part of the proprietor of the signals. They were designed to only view signals that were unscrambled and truly “free” in the air.

20. DISH Network generates its revenues through the sale of subscription programming packages, and as a result, DISH Network must be able to condition subscriber access to programming on the purchase of legitimate subscriptions. EchoStar Technologies generates revenues through the sale and/or lease of its equipment for the use of the legitimate subscribers of DISH Network services. Accordingly, DISH Network and EchoStar Technologies devote substantial resources to the continued development and improvement of their security system and related technologies.
21. By illicitly circumventing the Plaintiffs’ security measures, through piracy devices such as modified FTA receivers pirates gained unauthorized access to all of DISH Network’s programming, including premium and pay-per-view events, without paying for them. The aggregate purchase value of all illegally pirated programming available for illicit viewing at a single residence for one month could exceed thousands of dollars.
22. Satellite piracy damages DISH Network in that DISH Network does not obtain income from the signals received by individuals engaged in piracy. Satellite piracy also damages DISH Network ability to obtain and keep subscribers, and to protect and maintain its rights to distribute copyrighted and proprietary programming. Losses sustained by DISH Network from piracy result in otherwise unnecessary rate increases charged to DISH Network’s many honest subscribers despite its aforementioned security measures.
23. Satellite piracy damages EchoStar Technologies by depriving EchoStar Technologies of revenues derived from the sale and/or distribution of legitimate DISH Network hardware and by compromising EchoStar Technologies’ proprietary information, and by

interfering with EchoStar's contractual and prospective business relations.

The Defendant's Actions

24. On July 16, 2008 federal criminal authorities, including personnel from the Federal Bureau of investigation executed, search warrants at a residence in Paris, Texas, a business in Talihina, Texas, and a business in Hugo, Oklahoma. From this raid, the federal criminal authorities recovered a significant amount of sales records related to Mr. Charles Groome ("Groome") and his businesses, FTA Electronics and Hugo TV & Computer.
25. Groome was in the business of selling DISH Network piracy devices; he was selling modified FTA receivers, FTA receivers that had been programmed with modified FTA card hack software.
26. The Plaintiffs and an affiliate brought a civil action against Groome in Federal District Court for the Eastern District of Texas alleging that Groome was selling DISH Network piracy devices, modified FTA receivers. *DISH Network et al v Charles Groome*, 4:08-cv-00262-DDB; on or about February 3, 2010 the Plaintiffs prevailed in their claims against Groome by way of summary judgment and the final judgment was entered on March 5, 2010.
27. Groome was also the subject of federal criminal prosecution related to the sale of these devices in the Federal District Court for the Eastern District of Texas *US v Groom* 4:09-cr-00162-DF-ALM-1; on or about December 18, 2009 Groome was found guilty of these charges but he has yet to be sentenced.
28. The sales information obtained through the search warrants executed on Groome was ultimately shared with the Plaintiffs such that Plaintiffs came into possession of copies of records (the "Groome records"). In reliance upon those records and other information,

and upon information and belief, Plaintiffs have set forth the allegations in this Complaint.

29. Specifically, the Groome records indicate that:
 - a. The Defendant purchased a Neusat FTA receiver from Groome on or about April 29, 2007. In reliance upon those records and other information, and upon information and belief, Plaintiffs have set forth the allegations in this Complaint.
 - b. The Defendant paid Groome \$1,199.00 for the Neusat FTA receiver, a price indicative of the receiver having been programmed with modified FTA card hack software.
 - c. On or about May 4, 2007, there was a software update performed on the Neusat FTA receiver by Mr. Groome.
 - d. On or about July 4, 2007, there was a second software update performed on the Neusat FTA receiver by Mr. Groome.
 - e. At some point in time, the Defendant paid Mr. Groome \$125.00 for an upgrade to a SatPro FTA receiver.
 - f. On or about May 19, 2008, there was a software update performed on the SatPro FTA receiver by Mr. Groome.
30. Individuals who purchased modified FTA receivers from Groome would have the ability to utilize the modified FTA receivers to decrypt DISH Network's signals without authorization and without any payment to DISH Network.
31. The Defendant had been a paying subscriber of DISH Network but the Defendant terminated his account with DISH Network on or about May 12, 2007, shortly after he purchased his first device from Groome.
32. Based upon the fact that the Defendant had been a paying subscriber of DISH Network,

the Plaintiffs have thereby established the fact that at all times pertinent hereto the Defendant possessed the requisite digital satellite system hardware, including an EchoStar Technologies satellite antenna dish which would have allowed reception of the Plaintiffs' satellite television signals.

33. Individuals who purchased modified FTA receivers from Groome would have the ability to utilize the modified FTA receivers to decrypt DISH Network's signals without authorization.
34. On information and belief the Defendant obtained unauthorized access to DISH Network signals, including its premium and pay-per-view satellite television programming services without paying for the same while utilizing a modified FTA receiver.

COUNT I

UNAUTHORIZED RECEPTION OF SATELLITE SIGNALS IN VIOLATION OF 47 U.S.C. § 605(a)

35. The Plaintiffs, EchoStar Technologies and DISH Network, repeat and re-allege the allegations in Paragraphs 1 through 34 as if set forth fully herein.
36. On information and belief, the Defendants unlawfully received and intercepted, for their own use, DISH Network's satellite transmissions, including its premium and pay-per-view television programming, without authorization in violation of 47 U.S.C. § 605(a) by using a modified FTA receiver such that the Defendant could receive programming services without paying for them.
37. DISH Network's satellite transmissions of television programming constitute interstate or foreign "radio communications" and "direct-to-home satellite services" within the meaning of provisions of 47 U.S.C. § 605.
38. On information and belief, Defendant's violations of 47 U.S.C. § 605 have injured DISH

Network by depriving it of subscription and pay-per-view revenues and other valuable consideration by causing DISH Network to expend funds and effort on policing this piracy activity and by compromising the Plaintiffs' security and accounting systems.

39. On information and belief, Defendant's violations of 47 U.S.C. § 605 have injured EchoStar Technologies by depriving it of revenue through the sale and/or lease of legitimate equipment, by interfering with EchoStar Technologies' contractual and/or business relations with DISH Network by causing EchoStar Technologies to expend funds and effort on policing this piracy activity and by compromising EchoStar Technologies' security systems and by compromising the Plaintiffs' security and accounting systems.
40. DISH Network and EchoStar Technologies are "persons" aggrieved by the Defendant's violations of Title 47 U.S.C. § 605(a) and they are authorized to bring this action pursuant to Title 47 U.S.C. § 605 (e)(3)(A).

COUNT II

CIRCUMVENTION OF COPYRIGHT PROTECTION SYSTEMS IN VIOLATION OF 17 U.S.C. § 1201(a)(1)(A)

41. The Plaintiffs, EchoStar Technologies and DISH Network, allege and incorporate by reference Paragraphs 1 through 40 as if set forth fully herein.
42. On information and belief, the Defendant violated the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201(a)(1)(A), by directly or indirectly circumventing the technological protection measures used by the Plaintiffs to effectively control access to works protected under Title 17 of the United States Code, namely the satellite television programming and the protected works broadcasted thereon, in order to view such programming.

43. On information and belief, the Defendant's acts of circumvention were committed without the permission, authorization, or consent of EchoStar Technologies or DISH Network.
44. Defendant's conduct caused damage to the Plaintiffs.
45. EchoStar Technologies and DISH Network are "persons" aggrieved by the Defendant's violations of Title 17 U.S.C. § 1201(a)(1)(A) and they are authorized to bring this action pursuant to Title 47 U.S.C. § 1203(a).

COUNT III

INTERCEPTION OF TELECOMMUNICATION SERVICE (21 Okl. St. Ann. § 1737 *ET. SEQ.*)

46. The Plaintiffs, EchoStar Technologies and DISH Network, allege and incorporate by reference Paragraphs 1 through 45 as if set forth fully herein.
47. DISH Network's transmission, distribution, and sale of its satellite television signals is a "telecommunication service" as that term is utilized in 21 Okl. St. Ann. § 1737 .
48. On information and belief, the Defendant's unauthorized interception of DISH Network's signals is a violation of Oklahoma law, 21 Okl. St. Ann. § 1737 (1) which bars utilizing a device to obtain a telecommunications service without payment to the operator of said service.
49. On information and belief, the Defendant's actions in violation of Oklahoma statute referenced above have caused the Plaintiffs damage
50. DISH Network is a telecommunication service provider and EchoStar Technologies is a telecommunications equipment provider giving them standing to bring this action against the Defendant pursuant to 21 Okl. St. Ann. § 1737 (4) (c).

COUNT IV

UNJUST ENRICHMENT

51. The Plaintiff DISH Network alleges and incorporates by reference Paragraphs 1 through 50 as if set forth fully herein.
52. The Defendant has become enriched through the use of the modified FTA receiver in that he obtained DISH Network's satellite television programming for some considerable period of time without paying the Plaintiffs for the programming.
53. DISH Network suffered a loss based upon the Defendant's actions in that DISH Network did not receive any subscription or pay-per-view payments from the Defendant for any of the programming the Defendant obtained through the use of the modified FTA receiver.
54. The benefit the Defendant has received based upon his use of the modified FTA receiver is the value of the premium channels and pay-per-view events obtained as to which he made no payment to DISH Network.
55. It is contrary to equity and good conscience for the Defendant to retain the benefit which has come to him at the expense DISH Network.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiffs, DISH Network and EchoStar Technologies, request that this Court grant the following relief:

- (1) Find the Defendant's conduct:
 - a. In obtaining the DISH Network's signals and using same for his own benefit violated 47 U.S.C. § 605(a);
 - b. In utilizing a technological measure to circumvent the Plaintiffs' encryption technology to obtain copyright protected signals violates 17 U.S.C. § 1201 (a)(1)(A);

- c. In obtaining a communication service with a device without payment to DISH Network's violated 21 Okl. St. Ann. § 1737 (1);
- d. Give rise to the common law claim of unjust enrichment such that the Defendant should not be allowed to keep the benefit he obtained through acquiring DISH Network's signals without paying DISH Network for the signals.

(2) Statutory damages against the Defendant and in favor of the Plaintiffs for the Defendant's unauthorized interception of and personal use of the DISH Network's signals in violation of 47 U.S.C. § 605(a) of \$10,000.00 pursuant to 47 U.S.C. § 605(e)(3)(C)(i)(II) with the Plaintiffs reserving the right to:

- a. Later amend said statutory damage amount; and/or
- b. Claim actual damages under the statute.

(3) Statutory damages against the Defendant and in favor of the Plaintiffs for the Defendant's utilization of a technical measure to circumvent the Plaintiffs' encryption technology to obtain copyright protected signals in violation of 21 Okl. St. Ann. § 1737 (1) of \$2,500.00 pursuant to 21 Okl. St. Ann. § 1737 (4)(c)(1) with the Plaintiffs reserving the right to:

- a. Later amend said statutory damage amount; and/or
- b. Claim three times the actual damages pursuant to 21 Okl. St. Ann. § 1737 (4)(C)(2).

(4) Damages based upon the Defendant's unjust enrichment.

(5) The Plaintiffs' attorney's fees and costs in prosecuting this lawsuit as provided for by 47 U.S.C. § 605(e)(3)(B)(iii) and/or 17 U.S.C. § 1203(b)(4) and 17 U.S.C. § 1203(b)(5) and/or 21 Okl. St. Ann. § 1737 (4)(C)(2));

(6) The issuance of a permanent injunction pursuant to provisions of 47 U.S.C. § 605(e)(3)(B)(i) and/or 17 U.S.C. § 1203(b)(1) and/or 21 Okl. St. Ann. § 1737 (4)(D) utilizing the following language or language of a similar nature:

“The Court hereby enjoins the Defendant, the Defendant’s respective agents, servants, employees and any person or entity controlled directly or indirectly by the Defendants or acting on the Defendant’s behalf from the further use and/or distribution of electronic equipment designed for the unauthorized interception of telecommunications signals.


(7) Post judgment interest pursuant to 26 U.S.C. § 1961; and

(8) Such other and further relief as this Court may deem just and proper.

PLAINTIFFS’ DEMAND FOR JURY TRIAL

The Plaintiffs hereby assert their rights under the Seventh Amendment to the United States Constitution and demand, in accordance with FRCP 38 a trial by jury on all issues excepting the injunctive/equitable relief specifically sought above.

July 16, 2010.



Weldon Stout, OBA #8673
Justin Stout, OBA #91581
Wright, Stout & Wilburn, PLLC
300 W. Broadway
Muskogee, OK 74401
Telephone (918) 682-0091
Facsimile (918) 683-6341
Weldon@wsfw-ok.com